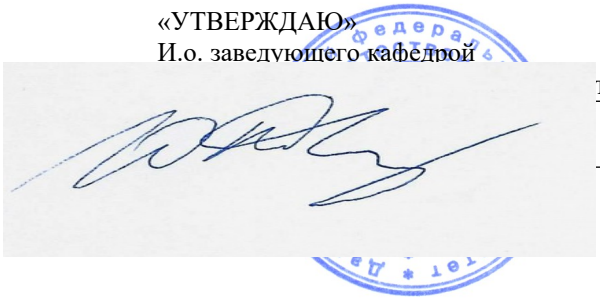
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет» (ДВФУ)
ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Варлатая С.К.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой



ти

Ю.В.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Теоретико-числовые методы в криптографии»
Направление подготовки 10.03.01 Информационная безопасность
(Комплексная защита объектов информатизации)
Форма подготовки очная

Школа естественных наук
Кафедра информационной безопасности
курс 4 семестр 7
лекции 00 час.
практические занятия 36 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 36 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 00 час.
контрольные работы (количество) 00
курсовая работа / курсовой проект не предусмотрены
зачет 7 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 10.03.01 **Информационная безопасность**, утвержденного приказом Министерства образования и науки РФ от __ _____ 20__г. №_____/ образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 7 от « 19 » июня 2019 г.

И.о. заведующего кафедрой : Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Дзенскевич Е.А., к.т.н., Захарченко Д.В., ассистент

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

Аннотация к рабочей программе дисциплины «Теоретико-числовые методы в криптографии»

Курс учебной дисциплины «Теоретико-числовые методы в криптографии» предназначен для обучения студентов направления 10.03.01 «Информационная безопасность», профиль «Комплексная защита объектов информатизации» и входит в состав факультативных дисциплин учебного плана ФТД.В.01.

Общая трудоемкость освоения дисциплины составляет 72 часов (2 з.е.). Учебным планом предусмотрены лекционные занятия (18 час.), лабораторные работы (18 час.), самостоятельная работа (36 час.). Дисциплина реализуется на 3 курсе в 5 и 6 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Теоретико-числовые методы в криптографии» логически и содержательно связана с такими курсами, как «Математическая логика и теория алгоритмов», «Теория информации», «Информатика», «Криптографические методы защиты информации».

Содержание дисциплины охватывает следующий круг вопросов: теоретико-числовые алгоритмы в криптографии, криптографические системы и их реализация.

Цель: изложение основ теории чисел и особенностей применения теоретико-числовых алгоритмов при построении криптографических систем.

Задачи:

- изучить основы теории чисел;
- изучить основы теории сложности алгоритмов;
- обозначить перспективы применения результатов теории чисел в криптографической защите информации.

Для успешного изучения дисциплины «Теоретико-числовые методы в криптографии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-8).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-2) Способностью применять соответствующий математический аппарат для решения профессиональных задач	Знает	Применения алгебры высказываний, теории булевых функций, алгебры предикатов, формализованного исчисления.
	Умеет	Использовать законы логики для проверки правильности суждений, решении логических задач, построении доказательств математических утверждений.
	Владеет	Навыками использования логических законов.
(ПК-2) способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает	модель перевода информации из одной формы в другую и источники ошибок в программном средстве
	Умеет	качественно и концептуально описывать процесс разработки программного средства для конкретной предметной задачи
	Владеет	общей подготовкой (базовыми знаниями) для решения практических задач в предметных областях средствами технологии программирования

Для формирования вышеуказанных компетенций в рамках дисциплины «Теоретико-числовые методы в криптографии» применяются следующие методы обучения: чтение лекций с использованием мультимедийного оборудования (проектор), проведение и сдача лабораторных работ. Используемые оценочные средства: конспект (ПР-7), лабораторные работы (ПР-6).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекционные занятия (18 часов)

Введение (1 час)

Основные понятия криптографии: криптография как наука, отличие от стеганографии, определения открытого текста, шифротекста, шифра и ключа, классификация шифров, примеры шифров. Основные понятия криптоанализа. Рекомендуемая литература.

Модуль 1. Основы теоретико-числовых методов в криптографии (8 часов)

Тема 1. Основы теории чисел

Делимость, простые числа и взаимно простые числа. Наибольший общий делитель и его линейное представление. Алгоритм Евклида, расширенный алгоритм Евклида. Функция Эйлера.

Тема 2. Теория сравнений. Вычеты

Свойства сравнений. Полная система вычетов, приведенная система вычетов. Обратный элемент. Теорема Эйлера, обобщенная теорема Эйлера. Теорема Ферма. Показатели и первообразные корни. Индексы по модулям, дискретный логарифм. Понижение степени сравнения.

Тема 3. Сравнения первой степени. Системы сравнений первой степени

Сравнения первой степени и их решение. Теоремы о числе классов с заданным показателем. Теоремы о числе решений степенных сравнений. Алгоритм быстрого возведения в степень по модулю. Системы сравнений первой степени и их решение. Китайская теорема об остатках и ее применения в криптографии. Криптосистема RSA.

Тема 4. Квадратичные сравнения. Теория квадратичных вычетов

Квадратичные сравнения. Критерий Эйлера. Символ Лежандра. Закон взаимности. Существование решений квадратичного сравнения по простому модулю. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства. Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных сравнений по составному модулю. Решение систем с квадратичными сравнениями. Извлечение квадратных корней по простому модулю. Извлечение корней степени $n>2$ по простому модулю. Извлечение корня в случае модуля, равного степени простого числа.

Трудные случаи извлечения корней по простому модулю: модуль со специальной структурой, вычисление корня большой простой степени, сведение трудных случаев извлечения корней к задаче дискретного логарифмирования.

Тема 5. Вероятностные тесты на простоту. Доказуемо простые и псевдопростые числа

Генерация простых чисел. Вероятностные тесты. Тест Ферма. Псевдопростые числа, числа Кармайкла, числа Ферма. Тест Соловея-Штрассена. Квадраты и псевдоквадраты. Тест Миллера-Рабина. Числа Блюма. Детерминистическая генерация больших простых чисел.

Модуль 2. Приложение теоретико-числовых методов в криптографии (8 часов)

Тема 1. Нахождение порождающих элементов
Циклическая группа Z^*_p (U_p). Нахождение первообразных корней. Нахождение чисел, относящихся к заданному простому показателю. Нахождение чисел, относящихся к заданному составному показателю.
Тема 2. Введение в теорию сложности алгоритмов. Факторизация. Дискретное логарифмирование
Элементы теории сложности. Оценки сложности по времени, по объему требуемой памяти. Полиномиальная сложность, субэкспоненциальная сложность, экспоненциальная сложность алгоритмов. Сложность элементарных опе раций. Теоретико-числовые проблемы, лежащие в основе двухключевых криптосистем - факторизация, дискретное логарифмирование.
Алгоритмы факторизации: факторизация B-гладкого модуля RSA, факто-ризация модуля RSA с использованием метода Флойда.
Методы дискретного логарифмирования: оптимизация переборного метода, метод вычисления индексов, метод Полларда, случай составного порядка.
Тема 3. Конечные группы и поля многочленов
Основные понятия алгебры. Группы, поля, кольца многочленов, конечные поля. Изоморфизм. Многочлены над Z_p, Z_n. Неприводимые многочлены, примитивные многочлены. Порядок элемента в конечном поле.
Операции над многочленами: Сложение многочленов, умножение многочленов, НОД многочленов, деление многочленов с остатком, разложение многочлена на множители над конечными полями.
Тема 4. Эллиптические кривые
Каноническая форма эллиптической кривой. Групповой закон. Сложение точек эллиптической кривой. Порядок эллиптической кривой. Теорема Хассе. Проективные координаты. Алгоритм быстрого умножения точки эллиптической кривой на число.
Заключение (1 час)
Подведение итогов курса. Краткий обзор современной криптографии.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные занятия (18 час.)

1. Применение основ теории чисел
2. Применение теории сравнений и систем вычетов
3. Решение сравнений первой степени и систем сравнений первой степени
4. Решение квадратичных сравнений и систем с квадратичными сравнениями
5. Решение задач по теории квадратичных вычетов
6. Применение вероятностных тестов на простоту. Изучение теории псевдопростых чисел
7. Решение задач по поиску порождающих элементов и чисел, относящихся к заданному показателю
8. Изучение и применение теории сложности алгоритмов

9. Решение задач с использованием алгебраических структур
10. Проведение расчетов с использованием эллиптических кривых

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Наука о данных и аналитика больших объемов данных» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Введение	ОПК-2 ПК-2	знает	ПР-7	1-3
			умеет	ПР-7	1-3
			владеет	ПР-7	1-3
2	Основы теоретико-числовых методов в криптографии	ОПК-2 ПК-2	знает	ПР-6	4-34
			умеет	ПР-6	4-34
			владеет	ПР-6	4-34
3	Приложение теоретико-числовых методов в криптографии	ОПК-2 ПК-2	знает	ПР-6	35-64
			умеет	ПР-6	35-64
			владеет	ПР-6	35-64
4	Заключение	ОПК-2 ПК-2	знает	ПР-7	65-67
			умеет	ПР-7	65-67

			владеет	ПР-7	65-67

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Ю. Л. Сагалович Введение в алгебраические коды: учебное пособие / Москва: Изд-во Института проблем передачи информации РАН, 2014. 310 с. Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:756734&theme=FEFU
2. Теоретико-числовые методы в криптографии [Электронный ресурс]: учебное пособие/ — Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2017.— 107 c URL: http://www.iprbookshop.ru/75601.html
   Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учебное пособие / М.М. Глухов [и др.]. — Электрон. дан. — Санкт-Петербург : Лань, 2011. — 400 с. URL: https://e.lanbook.com/book/68466

Дополнительная литература:

1. Ниссенбаум, О.В. Теоретико-числовые методы в криптографии. Сборник заданий (часть III) [Электронный ресурс] : учебно-методическое пособие / О.В. Ниссенбаум. — Электрон. дан. — Тюмень : , 2014. — 40 с. URL: https://e.lanbook.com/book/110138
2. Криптографические методы защиты информации.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 413 с. URL: http://znanium.com/catalog/product/960001

3. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 URL: http://znanium.com/catalog/product/441493
4. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс] : учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза : ПензГТУ, 2013. — 180 с. URL: https://e.lanbook.com/book/62755

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Важной является самостоятельная работа по курсу. В ходе этой работы студенты отбирают необходимый материал по изучаемому вопросу и анализируют его. Самостоятельная работа с литературой включает в себя написание рефератов.

Студентов необходимо познакомить с основными источниками, без которых невозможно полноценное понимание проблематики курса. Поэтому эти источники рекомендованы студентам для домашнего изучения и включены в программу.

Методические указания по сдаче зачета.

Зачеты принимаются ведущим преподавателем. При большом количестве групп у одного преподавателя или при большой численности потока по распоряжению заведующего кафедрой (заместителя директора филиала по учебной и воспитательной работе) допускается привлечение в помощь ведущему преподавателю других преподавателей.

Форма проведения зачета (устная, письменная и др.) утверждается на заседании кафедры по согласованию с руководителем в соответствии с рабочей программой учебной дисциплины.

Во время проведения зачета студенты могут пользоваться рабочей программой учебной дисциплины, а также с разрешения преподавателя, проводящего зачет, справочной литературой и другими пособиями (учебниками, учебными пособиями, рекомендованной литературой и т.п.).

Зачетные ведомости являются основными первичными документами по учету успеваемости студентов. Администраторы образовательных программ до начала процедуры приема зачетов и экзаменов формируют зачетно-экзаменационные ведомости.

При явке на экзамены и зачеты студенты обязаны иметь при себе зачетную книжку, которую они предъявляют экзаменатору.

Преподаватель заполняет соответствующие графы зачетной книжки студента, а именно: название дисциплины записывается полностью, без сокращений, в соответствии с учебным планом, также указывается фамилия преподавателя, оценка, дата, подпись, трудоемкость дисциплины, указанная в зачетно-экзаменационной ведомости или листе.

При промежуточной аттестации обучающимся устанавливаются оценки: по зачетам: «зачтено» и «не зачтено».

В зачетную книжку студента и в экзаменационную ведомость вносятся только положительные оценки, неудовлетворительные оценки вносятся только в экзаменационную ведомость. При заполнении ведомости не допускаются прочерки или незаполненные графы. Неявка студента на зачет без уважительной причины может быть засчитана как получение неудовлетворительной оценки, при этом в ведомости делается запись «не явился».

Оценки, выставленные экзаменатором по итогам зачетов, не подлежат пересмотру.

Студент, не согласный с выставленной оценкой, имеет право в течение следующего рабочего дня подать заявление, согласованное с руководителем ООП, на имя директора Школы (филиала) с просьбой о пересдаче экзамена комиссии. В случае обоснованности поданного заявления директор Школы

создает комиссию в составе не менее 3 профильных преподавателей по соответствующей кафедре. Оценка, полученная студентом во время пересдачи экзамена комиссии, является окончательной.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 738, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 208) Оборудование: "Мультимедийное оборудование: Экран проекционный Projecta Elpro Large Electrol, 500x316 см, размер рабочей области 490x306 Документ-камера Avervision CP 355 AF Мультимедийный проектор Panasonic PT-DZ11OXE, 10 600 ANSI Lumen, 1920x1200 Сетевая видеокамера Multipix MP-HD718 ЖК-панель 47"", Full HD, LG M4716 CCBA ЖК-панель 42"", Full HD, LG M4214 CCBA ЖК-панель 42"", Full HD, LG M4214 CCBA" Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет» (ДВФУ)
ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Теоретико-числовые методы в криптографии»
Направление подготовки 10.03.01 «Информационная безопасность»
(Комплексная защита объектов информатизации)
Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
Пятый семестр				
1	2 неделя	Работа с конспектом	27 часов	ПР-6
2	6 неделя	Работа с конспектом	27 часов	ПР-6
3	8 неделя	Работа с конспектом	27 часов	ПР-6
4	12 неделя	Работа с конспектом	27 часов	ПР-6
5	16 неделя	Зачет	18 часов	ПР-6
Шестой семестр				
1	2 неделя	Работа с конспектом	27 часов	ПР-6
2	6 неделя	Работа с конспектом	27 часов	ПР-6
3	8 неделя	Работа с конспектом	27 часов	ПР-6
4	12 неделя	Работа с конспектом	27 часов	ПР-6
5	16 неделя	Зачет	18 часов	ПР-6

Характеристика заданий для самостоятельной работы студентов и методические рекомендации по их выполнению

Самостоятельная работа помогает студентам:

1) овладеть знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы и т.д.);

- составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста и т.д.;

- работа со справочниками и др. справочной литературой;

- использование компьютерной техники и Интернета и др.;

2) закреплять и систематизировать знания:

- работа с конспектом лекции;

- обработка текста, повторная работа над учебным материалом учебника, первоисточника, дополнительной литературы, аудио и видеозаписей;

- подготовка плана;

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности и уровня умений студентов.

Контроль результатов самостоятельной работы студентов должен осуществляться в пределах времени, отведенного на обязательные учебные занятия и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Работа с литературными источниками

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой.

Требования к представлению и оформлению результатов самостоятельной работы

Требования к конспекту для практических занятий:

1. Должен быть в отдельной тетради, подписанный.

2. Обязательно писать план занятия с указанием темы, вопросов, списка литературы и источников.

3. Отражать проблематику всех поставленных вопросов (анализ источника, литературы).

4. Иметь по ним аргументированные выводы. Слово «аргументированные» является ключевым. Главное - доказуемость выводов.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы:

- Устный опрос.
- Зачет.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- сформированность общеучебных умений;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать ее.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет» (ДВФУ)
ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Теоретико-числовые методы в криптографии»
Направление подготовки 10.03.01 «Информационная безопасность»
(Комплексная защита объектов информатизации)
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-2) Способностью применять соответствующий математический аппарат для решения профессиональных задач	Знает	Применения алгебры высказываний, теории булевых функций, алгебры предикатов, формализованного исчисления.
	Умеет	Использовать законы логики для проверки правильности суждений, решении логических задач, построении доказательств математических утверждений.
	Владеет	Навыками использования логических законов.
(ПК-2) способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает	модель перевода информации из одной формы в другую и источники ошибок в программном средстве
	Умеет	качественно и концептуально описывать процесс разработки программного средства для конкретной предметной задачи
	Владеет	общей подготовкой (базовыми знаниями) для решения практических задач в предметных областях средствами технологии программирования

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Введение	ОПК-2 ПК-2	знает	ПР-7	1-3
			умеет	ПР-7	1-3
			владеет	ПР-7	1-3
2	Основы теоретико-числовых методов в криптографии	ОПК-2 ПК-2	знает	ПР-6	4-34
			умеет	ПР-6	4-34
			владеет	ПР-6	4-34
3	Приложение теоретико-числовых методов в криптографии	ОПК-2 ПК-2	знает	ПР-6	35-64
			умеет	ПР-6	35-64
			владеет	ПР-6	35-64
4	Заключение	ОПК-2 ПК-2	знает	ПР-7	65-67
			умеет	ПР-7	65-67
			владеет	ПР-7	65-67

Оценочные средства для промежуточной аттестации

Устный ответ:

1. 100-85 баллов - если ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

2. 85-76 - баллов - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3. 75-61 - балл – оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

4. 60-50 баллов – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы,

слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Вопросы к зачету

1. Основные понятия теории чисел. Теорема делимости.
2. Наибольший общий делитель и алгоритм Евклида.
3. Цепные дроби и алгоритм Евклида.
4. Наименьше общее кратное. Простые числа.
5. Теоремы Евклида о простых числах. Решето Эратосфена.
6. Основные свойства простых чисел. Теорема о единственности разложения на простые сомножители.
7. Теорема о делителях числа и ее следствия.
8. Асимптотический закон распределения простых чисел.
9. Функция Эйлера, ее свойства.
10. Сравнения. Свойства сравнений.
11. Полная система вычетов, приведенная система вычетов. Алгебраические свойства, обратный элемент.
12. Теорема Эйлера, теорема Ферма. Следствие.
13. Тест Ферма на простоту. Числа Кармайкла. Теорема Кармайкла.
14. Применение теоремы Ферма в криптосистеме RSA.
15. Сравнения с одним неизвестным 1-й степени.
16. Система сравнений 1-й степени. Китайская теорема об остатках.
17. Применение Китайской теоремы об остатках в RSA и схема разделения секрета на ее основе.
18. Квадратичные сравнения попростому модулю.
19. Символ Лежандра и его свойства.
20. Решение квадратичных сравнений по простому модулю.
21. Число решений квадратичного сравнения по составному модулю.
22. Символ Якоби, его свойства. Тест Соловея-Штрассена.

23. Квадратичные сравнения по модулю RSA. Связь задач извлечения

24. Тест Миллера-Рабина.

25. Порядок группы. Порядок элемента в группе. Порождающий элемент.

26. Существование порождающего элемента в Z*n

27. Критерий Люка.

28. Теорема Сэлфриджа и тест Миллера.

29. Теорема Поклнгтонаи тест на простоту на ее основе.

30. Числа Ферма, теорема Пепина, тест Пепина.

31. Числа Мерсена. Тест Лукаса-Лемера.

32. Теорема Диемитко. Процедура генерации простых чисел

33. Дискретный логарифм. Проблема Диффи-Хелмана. Криптосистема ЭльГамаля.

34. Кольца многочленов.